IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 January 2024, accepted 29 January 2024, date of publication 5 February 2024, date of current version 14 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3361921

RESEARCH ARTICLE

A New PUF-Based Protocol for Mutual Authentication and Key Agreement Between Three Layers of Entities in Cloud-Based IoMT Networks

AMIR MASOUD AMINIAN MODARRES[1], **NIMA S. ANZABI-NEZHAD**[2], **AND MARYAM ZARE**[2]

[1]Department of Electrical Engineering, Sadjad University, Mashhad 9188148848, Iran
[2]Department of Electrical Engineering, Faculty of Electrical and Computer Engineering, Quchan University of Technology, Quchan 9477177870, Iran

Corresponding author: Amir Masoud Aminian Modarres (am_aminian@sadjad.ac.ir)

ABSTRACT The Internet of Medical Things (IoMT) is a promising framework for expanding and improving telemedicine services. A common cloud-based IoMT architecture consists of three layers of entities, the first layer (such as smart sensors and devices), the second layer (such as gateways), and the third layer (such as cloud servers). Obviously, in these networks, the protection of sensitive information against security threats as well as authentication between the entities is a key issue. On the other hand, the devices involved in the first and second layers usually suffer from poor computational capabilities as well as a lack of physical protection, which should be considered in the design of security protocols. Recently, Alladi et al. have proposed a lightweight authentication protocol for the cloud-based IoMT that addresses these challenges, using Physically Unclonable Function (PUF). In this paper, we first provide thorough cryptanalysis of their scheme and clarify its important vulnerabilities that lead to protocol collapse. Then, we propose a new lightweight protocol based on PUF to perform strong mutual authentication and key agreement between parties in the IoMT networks. The formal (using BAN logic) and informal security analysis demonstrate that our scheme is resistant to several well-known attacks, including physical attacks. Also, our evaluation of computational cost and security features clearly shows that the proposed scheme outperforms similar schemes in security and efficiency. Another important advantage of our protocol is that it performs the mutual authentication and key agreement process separately for each pair of layers in the three-layer cloud-based IoMT architecture. This triple authentication scheme provides the necessary flexibility for use in different scenarios and working conditions. In this aspect, as far as we know, our proposed protocol is the first of its kind.

INDEX TERMS Authentication protocol, Internet of Medical Things (IoMT), network security, physically unclonable function (PUF), physical attacks.

I. INTRODUCTION

It has been more than twenty years since the term ‘‘Internet of Things’’ (IoT) was first introduced by Ashton et al. [1]. Recent developments in hardware design and information and communication technology (ICT) have led to billions of interconnected intelligent devices in basic infrastructures such as industrial automation, home automation, vehicle automation, unmanned aerial vehicles (UAVs), healthcare systems, environmental control systems, and smart cities [2]. The size of the global IoT market has grown exponentially over the past decade, and with this growth rate, it will increase from an estimated 157 billion USD in 2016 to an expected 771 billion USD by 2026 [3]. Nowadays, a new and evolving generation of the Internet of Things called IoT 2.0 is emerging, in which the IoT is integrated with other modern technologies such as 5G communication, Tactile Internet, artificial intelligence, big data, edge computing,

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Sharif.